

BackTrack 4 Beta

The Perfect Hard Disk Install v2

muts@remote-exploit.org

BackTrack 4 Beta does not contain an installer in it yet. We've compiled this cookbook for getting the "perfect" BT4 install up and running quickly. The assumption is that you are installing BT4 on an empty disk (/dev/sda in our case). Make sure to adjust this accordingly if needed.

1. Start by partitioning the disk. Create 3 partitions for boot, swap and root.

```
root@bt:~# fdisk /dev/sda
```

```
The number of cylinders for this disk is set to 1044.
```

```
There is nothing wrong with that, but this is larger than 1024,  
and could in certain setups cause problems with:
```

- 1) software that runs at boot time (e.g., old versions of LILO)
- 2) booting and partitioning software from other OSs
(e.g., DOS FDISK, OS/2 FDISK)

```
Command (m for help): n
```

```
Command action
```

```
  e   extended
```

```
  p   primary partition (1-4)
```

```
P
```

```
Partition number (1-4): 1
```

```
First cylinder (1-1044, default 1):
```

```
Using default value 1
```

```
Last cylinder, +cylinders or +size{K,M,G} (1-1044, default 1044): +128M
```

```
Command (m for help): n
```

```
Command action
```

```
  e   extended
```

```
  p   primary partition (1-4)
```

```
P
```

```
Partition number (1-4): 2
```

```
First cylinder (10-1044, default 10):
```

```
Using default value 10
```

```
Last cylinder, +cylinders or +size{K,M,G} (10-1044, default 1044): +1024M
```

```
Command (m for help): n
```

```
Command action
```

```

    e   extended
    p   primary partition (1-4)
P
Partition number (1-4): 3
First cylinder (142-1044, default 142):
Using default value 142
Last cylinder, +cylinders or +size{K,M,G} (142-1044, default 1044):
Using default value 1044

Command (m for help): t
Partition number (1-4): 2
Hex code (type L to list codes): 82
Changed system type of partition 2 to 82 (Linux swap / Solaris)

Command (m for help): a
Partition number (1-4): 1

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
root@bt:~#

```

2. Format the file systems, mount them and copy over the directory structure. Chroot into new environment.

```

root@bt:~# mke2fs /dev/sda1
root@bt:~# mkswap /dev/sda2
root@bt:~# swapon /dev/sda2
root@bt:~# mkreiserfs /dev/sda3
root@bt:~# mkdir /mnt/bt
root@bt:~# mount /dev/sda3 /mnt/bt/
root@bt:~# mkdir /mnt/bt/boot
root@bt:~# mount /dev/sda1 /mnt/bt/boot
root@bt:~# cp --preserve -R \
/{bin,dev,home,pentest,root,usr,boot,etc,lib,opt,sbin,var} /mnt/bt/
root@bt:~# mkdir /mnt/bt/{mnt,tmp,proc,sys}
root@bt:~# chmod 1777 /mnt/bt/tmp/
root@bt:~# mount -t proc proc /mnt/bt/proc
root@bt:~# mount -o bind /dev /mnt/bt/dev/
root@bt:~# chroot /mnt/bt/ /bin/bash

```

3. Configure /etc/lilo.conf to reflect your setup.

```
boot=/dev/sda
root=/dev/sda3

# bitmap=/boot/sarge.bmp
# bmp-colors=1,,0,2,,0
# bmp-table=120p,173p,1,15,17
# bmp-timer=254p,432p,1,0,0
# install=bmp

# delay=20

prompt
timeout=50

# map=/boot/map

vga=0x317

image=/boot/vmlinuz
    label="BT4"
    read-only
    initrd=/boot/splash.initrd
    append=quiet
```

4. Fix first line in `/etc/fstab`, and remove unnecessary mount lines. Add the swap partition to the `fstab` so it gets loaded at boot time. Your `fstab` should look similar to this:

```
/dev/sda3 / reiserfs defaults 0 0 # AutoUpdate
/dev/sda2 none swap sw 0 0
proc /proc proc defaults 0 0 # AutoUpdate
sysfs /sys sysfs defaults 0 0 # AutoUpdate
devpts /dev/pts devpts gid=5,mode=620 0 0 # AutoUpdate
tmpfs /dev/shm tmpfs defaults 0 0 # AutoUpdate
```

5. Execute `lilo` and reboot!

```
root@bt:/# lilo -v
LILO version 22.8, Copyright (C) 1992-1998 Werner Almesberger
Development beyond version 21 Copyright (C) 1999-2006 John Coffman
Released 19-Feb-2007, and compiled at 14:08:06 on May 15 2008
Ubuntu

Reading boot sector from /dev/sda
Using MENU secondary loader
Calling map_insert_data

Boot image: /boot/vmlinuz
Mapping RAM disk /boot/splash.initrd
Added BT4 *

Writing boot sector.
Backup copy of boot sector in /boot/boot.0800
root@bt:/# exit
exit
root@bt:~# reboot
```